

VISIT...

LANZAROTE
Caliente.COM

Ubervveillance and the Social Implications of Microchip Implants: Emerging Technologies

M.G. Michael
University of Wollongong, Australia

Katina Michael
University of Wollongong, Australia

A volume in the Advances in Human and
Social Aspects of Technology (AHSAT)
Book Series

Information Science
REFERENCE

An Imprint of IGI Global

Managing Director:	Lindsay Johnston
Production Manager:	Jennifer Yoder
Development Editor:	Joel Gamon
Acquisitions Editor:	Kayla Wolfe
Typesetter:	Christina Henning
Cover Design:	Jason Mull

Published in the United States of America by
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: <http://www.igi-global.com>

Copyright © 2014 by IGI Global. All rights reserved. No part of this publication may be reproduced, stored or distributed in any form or by any means, electronic or mechanical, including photocopying, without written permission from the publisher. Product or company names used in this set are for identification purposes only. Inclusion of the names of the products or companies does not indicate a claim of ownership by IGI Global of the trademark or registered trademark.

Library of Congress Cataloging-in-Publication Data

Uberveillance and the social implications of microchip implants: emerging technologies / M.G. Michael and Katina Michael, editors.

pages cm

Includes bibliographical references and index.

Summary: "This book presents case studies, literature reviews, ethnographies, and frameworks supporting the emerging technologies of RFID implants while also highlighting the current and predicted social implications of human-centric technologies"-- Provided by publisher.

ISBN 978-1-4666-4582-0 (hardcover) -- ISBN 978-1-4666-4583-7 (ebook) -- ISBN 978-1-4666-4584-4 (print & perpetual access) 1. Electronic surveillance--Social aspects. 2. Privacy, Right of--Social aspects. 3. Radio frequency identification systems. 4. Implants, Artificial. I. Michael, M. G. II. Michael, Katina, 1976-
HM846.U24 2014
323.44'82--dc23

2013020727

This book is published in the IGI Global book series Advances in Human and Social Aspects of Technology (AHSAT) (ISSN: 2328-1316; eISSN: 2328-1324)

British Cataloguing in Publication Data

A Cataloguing in Publication record for this book is available from the British Library.

All work contributed to this book is new, previously-unpublished material. The views expressed in this book are those of the authors, but not necessarily of the publisher.

For electronic access to this publication, please contact: eresources@igi-global.com.

Detailed Table of Contents

Foreword.....	xviii
Preface.....	xxiii
Acknowledgment.....	xl

Section 1 The Veillances

Chapter 1

Introduction: On the “Birth” of Uberveillance	1
<i>M. G. Michael, University of Wollongong, Australia</i>	

When or how *uberveillance* will be implemented in its full-blown manifestation is still a subject for some intriguing discussion and a topic of robust disagreement, but what is generally accepted by most of the interlocutors is that an “uberveillance society” will emerge sooner rather than later, and that one way or another this will mean an immense upheaval in all of our societal, business, and government relationships. What is apparent from the numerous qualitative and quantitative studies conducted is that microchipping people is a discernibly divisive issue. If we continue on the current trajectory, we will soon see further divisions – not just between those who have access to the Internet and those who do not, but between those who subjugate themselves to be physically connected to the Web of Things and People, and those who are content enough to simply have Internet connectivity through external devices like smart phones, to those who opt to live completely off the grid. Time will only tell how we as human-beings will adapt after we willingly adopt innovations with extreme and irreversible operations. This introduction serves to provide a background context for the term *uberveillance*, which has received significant international attention since its establishment.

Chapter 2

Veillance: Beyond Surveillance, Dataveillance, Uberveillance, and the Hypocrisy of One-Sided Watching	32
<i>Steve Mann, University of Toronto, Canada</i>	

This chapter builds upon the concept of Uberveillance introduced in the seminal research of M. G. Michael and Katina Michael in 2006. It begins with an overview of *sousveillance* (underwatching) technologies and examines the “*We’re watching you but you can’t watch us*” hypocrisy associated with the rise of *surveillance* (overwatching). Surveillance cameras are often installed in places that have “NO

CAMERAS” and “NO CELLPHONES IN STORE, PLEASE!” signage. The authors consider the chilling effect of this veillance hypocrisy on LifeGlogging, wearable computing, “Sixth Sense,” AR Glass, and the Digital Eye Glass vision aid. If surveillance gives rise to hypocrisy, then to what does its inverse, sousveillance (wearable cameras, AR Glass, etc.), give rise? The opposite (antonym) of *hypocrisy* is *integrity*. How might we resolve the conflict-of-interest that arises in situations where, for example, police surveillance cameras capture the only record of wrongdoing by the police? Is sousveillance the answer or will centralized dataveillance merely turn sousveillance into a corruptible *uberveillance* authority?

Chapter 3

Ubervveillance: Where Wear and Educative Arrangement	46
<i>Alexander Hayes, University of Wollongong, Australia</i>	

The intensification and diversification of surveillance in recent decades is now being considered within a contemporary theoretical and academic framework. The ambiguity of the term ‘surveillance’ and the surreptitiousness of its application must now be re-considered amidst the emergent concept of Ubervveillance. This chapter presents three cases of organisations that are currently poised or already engaging in projects using location-enabled point-of-view wearable technologies. Reference is made to additional cases, project examples, and testimonials including the Australian Federal Police, Northern Territory Fire Police and Emergency Services, and other projects funded in 2010 and 2011 by the former Australian Flexible Learning Framework (AFLF), now the National VET E-learning Strategy (NVELS). This chapter also examines the use of location-enabled POV (point-of-view) or Body Wearable Video (BWV) camera technologies in a crime, law, and national security context, referencing cross-sectoral and inter-disciplinary opinions as to the perceived benefits and the socio-technical implications of these pervasive technologies.

Section 2 Applications of Humancentric Implantables

Chapter 4

Practical Experimentation with Human Implants	64
<i>Kevin Warwick, University of Reading, UK</i>	
<i>Mark N. Gasson, University of Reading, UK</i>	

In this chapter, the authors report on several different types of human implants with which the authors have direct, first hand, experience. An indication is given of the experimentation actually carried out and the subsequent immediate consequences are discussed. The authors also consider likely uses and opportunities with the technology should it continue to develop along present lines and the likely social pressures to adopt it. Included in the chapter is a discussion of RFID implants, tracking with implants, deep brain stimulation, multi-electrode array neural implants, and magnetic implants. In each case, practical results are presented along with expectations and experiences.

Chapter 5

Knowledge Recovery: Applications of Technology and Memory	125
<i>Maria Burke, University of Salford, UK</i>	
<i>Chris Speed, University of Edinburgh, UK</i>	

The ability to “write” data to the Internet via tags and barcodes offers a context in which objects will increasingly become a natural extension of the Web, and as ready as the public was to adopt cloud-based services to store address books, documents, photos, and videos, it is likely that we will begin associat-

ing data with objects. Leaving messages for loved ones on a tea cup, listening to a story left on a family heirloom, or associating a message with an object to be passed on to a stranger. Using objects as tangible links to data and content on the Internet is predicted to become a significant means of how we interact with the interface of things, places, and people. This chapter explores this potential and focuses upon three contexts in which the technology is already operating in order to reflect upon the impact that the technology process may have upon social processes. These social processes are knowledge browsing, knowledge recovery, and knowledge sharing.

Section 3 Adoption of RFID Implants for Humans

Chapter 6

Willingness to Adopt RFID Implants: Do Personality Factors Play a Role in the Acceptance of Ubervveillance? 136

Christine Perakslis, Johnson and Wales University, USA

This chapter presents the results of research designed to investigate differences between and among personality dimensions as defined by Typology Theory using the Myers-Briggs Type Indicator (MBTI). The study took into account levels of willingness toward implanting an RFID (Radio Frequency Identification) chip in the body (ubervveillance) for various reasons including the following: to reduce identity theft, as a lifesaving device, for trackability in case of emergency, as a method to increase safety and security, and to speed up the process at airport checkpoints. The study was conducted with students at two colleges in the Northeast of the United States. The author presents a brief literature review, key findings from the study relative to personality dimensions (extroversion vs. introversion dimensions, and sensing vs. intuition dimensions), a discussion on possible implications of the findings when considered against the framework of Rogers' (1983; 2003) Diffusion of Innovation Theory (DoI), and recommendations for future research. A secondary, resultant finding reveals frequency changes between 2005 and 2010 relative to the willingness of college students to implant an RFID chip in the body. Professionals working in the field of emerging technologies could use these findings to better understand personality dimensions based on MBTI and the possible affect such personality dimensions might have on the process of adoption of such technologies as ubervveillance.

Chapter 7

Surveilling the Elderly: Emerging Demographic Needs and Social Implications of RFID Chip Technology Use 159

Randy Basham, University of Texas – Arlington, USA

This chapter describes the usefulness of RFID (Radio Frequency Identification Device) implant technology to monitor the elderly, who are aging in place in various retirement arrangements, and who need to maintain optimal functioning in the absence of available, and on location, service or care providers. The need to maintain functioning or sustainable aging is imperative for countries experiencing rapid growth as a demographic trend for the elderly. The chapter also raises some concerns including the social acceptance or rejection of RFID implant technology, despite the utility of the device. These concerns include a variety of political, social, and religious issues. Further, the chapter also attempts to show how RFID implant technology could be used in combination with other emerging technologies to maintain physical, emotional, and social functioning among the growing population of elderly. What follows is the introduction and a partial literature review on emergent elderly needs, and on the utilization of RFID and other technologies.

Section 4

Tracking and Tracing Laws, Directives, Regulations, and Standards

Chapter 8

Towards the Blanket Coverage DNA Profiling and Sampling of Citizens in England, Wales, and Northern Ireland 177

Katina Michael, University of Wollongong, Australia

The European Court of Human Rights (ECtHR) ruling of *S and Marper v United Kingdom* will have major implications on the retention of Deoxyribonucleic Acid (DNA) samples, profiles, and fingerprints of innocents stored in England, Wales, and Northern Ireland. In its attempt to develop a comprehensive National DNA Database (NDNAD) for the fight against crime, the UK Government has come under fire for its blanket-style coverage of the DNA sampling of its populace. Figures indicate that the UK Government retains a highly disproportionate number of samples when compared to other nation states in the Council of Europe (CoE), and indeed anywhere else in the world. In addition, the UK Government also retains a disproportionate number of DNA profiles and samples of specific ethnic minority groups such as the Black Ethnic Minority group (BEM). Finally, the *S and Marper* case demonstrates that innocent children, and in general innocent citizens, are still on the national DNA database, sometimes even without their knowledge. Despite the fact that the *S and Marper* case concluded with the removal of the biometric data of Mr S and Mr Marper, all other innocent subjects must still apply to their local Metropolitan Police Service to have their fingerprints or DNA removed from the register. This is not only a time-consuming process, but not feasible.

Chapter 9

ID Scanners and Überveillance in the Night-Time Economy: Crime Prevention or Invasion of Privacy?..... 198

Darren Palmer, Deakin University, Australia

Ian Warren, Deakin University, Australia

Peter Miller, Deakin University, Australia

ID scanners are promoted as a prominent solution to the problems of anti-social behavior and violence in many urban nighttime economies. However, the acceptance of this and other forms of computerized surveillance to prevent crime and anti-social behavior is based on several unproven assumptions. After outlining what ID scanners are and how they are becoming a normalized precondition of entry into one Australian nighttime economy, this chapter demonstrates how technology is commonly viewed as the key to preventing crime despite recognition of various problems associated with its adoption. The implications of technological determinism amongst policy makers, police, and crime prevention theories are then critically assessed in light of several issues that key informants talking about the value of ID scanners fail to mention when applauding their success. Notably, the broad, ill-defined, and confused notion of “privacy” is analyzed as a questionable legal remedy for the growing problems of überveillance.

Chapter 10

Global Tracking Systems in the Australian Interstate Trucking Industry 216

Jann Karp, C.C.C. Australia, Australia

Technology, trucking, and the surveillance of workers in the workplace: helpful or a hindrance? Technological advances are produced by the creative ideas individuals: these ideas then become selling items in their own right. Do tracking devices effectively regulate traffic breaches and criminality within the trucking industry? The data collection was conducted in the field while the authors rode as a passenger

with truck drivers on long-haul trips. The complexities of tracking systems became more apparent as the authors listened to the men and placed their narratives in a broader context for a broader audience. The results of the work indicated that the Global Positioning System (GPS) has a role in the management of the industry as a logistics tool, but that there are limitations to the technology. The drivers use the devices and also feel the oppressive oversight when managers use the data as a disciplinary tool.

Chapter 11

Tracking Legislative Developments In Relation To “Do Not Track” Initiatives 225

Brigette Garbin, University of Queensland, Australia

Kelly Staunton, University of Queensland, Australia

Mark Burdon, University of Queensland, Australia

Online behavioural profiling has now become an industry that is worth billions of dollars throughout the globe. The actual practice of online tracking was once limited to individual Websites and individual cookies. However, the development of new technologies has enabled marketing corporations to track the Web browsing activities of individual users across the Internet. Consequently, it should be no surprise that legislative initiatives are afoot throughout the world including the United States (US), the European Union (EU), and Australia. These different jurisdictions have put forward different methods of regulating online behavioural profiling and Do Not Track initiatives. Accordingly, this chapter overviews legislative developments and puts forward a typology of different legislative initiatives regarding the regulation of online behavioral profiling and Do Not Track issues. Particular focus is given to the Australian situation and whether existing Australian privacy law is sufficient to protect the privacy interests of individuals against the widespread use of online behaviour profiling tools.

Chapter 12

Ubervveillance, Standards, and Anticipation: A Case Study on Nanobiosensors in U.S. Cattle 250

Kyle Powys Whyte, Michigan State University, USA

Monica List, Michigan State University, USA

John V. Stone, Michigan State University, USA

Daniel Grooms, Michigan State University, USA

Stephen Gasteyer, Michigan State University, USA

Paul B. Thompson, Michigan State University, USA

Lawrence Busch, Michigan State University, USA

Daniel Buskirk, Michigan State University, USA

Erica Giorda, Michigan State University, USA

Hilda Bouri, Michigan State University, USA

Ubervveillance of humans will emerge through embedding chips within nonhumans in order to monitor humans. The case explored in this chapter involves the development of nanotechnology and biosensors for the real-time tracking of the identity, location, and properties of livestock in the U.S. agrifood system. The primary method for research on this case was an expert forum. Developers of biosensors see the tracking capabilities as empowering users to control some aspects of a situation that they face. Such control promises to improve public health, animal welfare, and/or economic gains. However, the ways in which social and ethical frameworks are built into standards for the privacy/access, organization, adaptability, and transferability of data are crucial in determining whether the diverse actors in the supply chain will embrace nanobiosensors and advance the ideals of the developers. Further research should be done that explores the possibilities of tripartite standards regimes and sousveillance in relation to nanobiosensors in agrifood.

Section 5

Health Implications of Microchipping Living Things

Chapter 13

Microchip-Induced Tumors in Laboratory Rodents and Dogs: A Review of the Literature 1990–2006.....	271
<i>Katherine Albrecht, CASPIAN Consumer Privacy, USA</i>	

This chapter reviews literature published in oncology and toxicology journals between 1990 and 2006 addressing the effects of implanted radio-frequency (RFID) microchips on laboratory rodents and dogs. Eleven articles were reviewed in all, with eight investigating mice and rats, and three investigating dogs. In all but three of the articles, researchers observed that malignant sarcomas and other cancers formed around or adjacent to the implanted microchips. The tumors developed in both experimental and control animals and in two household pets. In nearly all cases, researchers concluded that the microchips had induced the cancers. Possible explanations for the tumors are explored, and a set of recommendations for policy makers, human patients and their doctors, veterinarians, pet owners, and oncology researchers is presented in light of these findings.

Section 6

Socio-Ethical Implications of RFID Tags and Transponders

Chapter 14

Privacy and Pervasive Surveillance: A Philosophical Analysis	309
<i>Alan Rubel, University of Wisconsin – Madison, USA</i>	

This chapter analyzes some tools of pervasive surveillance in light of the growing philosophical literature regarding the nature and value of privacy. It clarifies the conditions under which a person can be said to have privacy, explains a number of ways in which particular facets of privacy are morally weighty, and explains how such conceptual issues may be used to analyze surveillance scenarios. It argues that in many cases, surveillance may both increase and decrease aspects of privacy, and that the relevant question is whether those privacy losses (and gains) are morally salient. The ways in which privacy diminishment may be morally problematic must be based on the value of privacy, and the chapter explains several conceptions of such values. It concludes with a description of how some surveillance technologies may conflict with the value of privacy.

Chapter 15

Neuroethics and Implanted Brain Machine Interfaces	338
<i>Ellen M. McGee, Independent Researcher, USA</i>	

Transformations of humans through advances in bioelectronics, nanotechnologies, and computer science are leading to hybrids of humans and machines. Future brain-machine interfaces will enable humans not only to be constantly linked to the Internet, and to cyber think, but will also enable technology to take information directly from the brain. Brain-computer interfaces, where a chip is implanted in the brain, will facilitate a tremendous augmentation of human capacities, including the radical enhancement of the human ability to remember and to reason, and to achieve immortality through cloning and brain downloading, or existence in virtual reality. The ethical and legal issues raised by these possibilities represent global challenges. The most pressing concerns are those raised by privacy and autonomy. The

potential exists for control of persons, through global tracking, by actually “seeing” and “hearing” what the individual is experiencing, and by controlling and directing an individual’s thoughts, emotions, moods, and motivations. Public dialogue must be initiated. New principles, agencies, and regulations need to be formulated and scientific organizations, states, countries, and the United Nations must all be involved.

Chapter 16

We Are the Borg! Human Assimilation into Cellular Society 353

Ronnie D. Lipschutz, University of California, USA

Rebecca Hester, University of Texas, USA

As cybersurveillance, datamining, and social networking for security, transparency, and commercial purposes become more ubiquitous, individuals who use and rely on various forms of electronic communications are being absorbed into a new type of cellular society. The eventual end of this project might be a world in which each individual, each cell in the electronic “body politic,” can be monitored, managed, and, if dangerous to the social organism, eliminated. This chapter examines the objectives, desires, and designs associated with such a cellular biopolitics. Are individuals being incorporated into a Borg-like cyber-organism in which they no longer “own” their substance, preferences, desires, and thoughts and in which they are told what they should be doing next?

Chapter 17

Uberveillance and Faith-Based Organizations: A Renewed Moral Imperative 393

Marcus Wigan, Oxford Systematics, Australia & Edinburgh Napier University, UK

Uberveillance extends the responsibilities of faith-based organisations to the power imbalances now emerging. This is less a matter of governance and strategy, and more one of the core values of faith-based organisations. These might be regarded from an ethical or moral standpoint, but the approach taken is to focus on the constituencies of faith-based organisations and the imperatives that have been woven into their aims and values. The specific ways in which such disempowerments emerge and the functional importance of making organizational responses are considered. Acknowledgement is made of the Science and Society Council of the Churches of Scotland, who catalysed the expression and articulation of these issues.

Glossary 402

Compilation of References 405

About the Contributors 436

Index..... 448

Chapter 2

Veillance:

Beyond Surveillance, Dataveillance, Uberveillance, and the Hypocrisy of One-Sided Watching

Steve Mann
University of Toronto, Canada

ABSTRACT

This chapter builds upon the concept of Uberveillance introduced in the seminal research of M. G. Michael and Katina Michael in 2006. It begins with an overview of sousveillance (underwatching) technologies and examines the “We’re watching you but you can’t watch us” hypocrisy associated with the rise of surveillance (overwatching). Surveillance cameras are often installed in places that have “NO CAMERAS” and “NO CELLPHONES IN STORE, PLEASE!” signage. The author considers the chilling effect of this veillance hypocrisy on LifeGlogging, wearable computing, “Sixth Sense,” AR Glass, and the Digital Eye Glass vision aid. If surveillance gives rise to hypocrisy, then to what does its inverse, sousveillance (wearable cameras, AR Glass, etc.), give rise? The opposite (antonym) of hypocrisy is integrity. How might we resolve the conflict-of-interest that arises in situations where, for example, police surveillance cameras capture the only record of wrongdoing by the police? Is sousveillance the answer or will centralized dataveillance merely turn sousveillance into a corruptible uberveillance authority?

INTRODUCTION: SURVEILLANCE

It is often said that we live in a “surveillance society” (Lyon, 2001), but what does “surveillance” mean? The primary definition of the word “surveillance” is:

sur-veil-lance [ser-vey-luhns] noun

1. *A watch kept over a person, group, etc., especially over a suspect, prisoner, or the like ...*

[examples] The suspects were under police surveillance. (Random House Dictionary, © Random House, Inc. 2013, accessed through dictionary.com)

DOI: 10.4018/978-1-4666-4582-0.ch002

Veillance

The word “surveillance” is from the French word “surveiller” which means “to watch over”. Specifically, the word “surveillance” is formed from two parts:

1. The French prefix “sur” which means “over” or “from above”; and
2. The French word “veillance” which means “watching” or “monitoring”

The word “Veillance” comes from the French word “veiller” which means “to watch”. It derives from the word “vigil”.

The Harper Collins Complete and Unabridged English Dictionary defines “vigil” as:

1. A purposeful watch maintained, esp at night, to guard, observe, pray, etc.;
2. The period of such a watch

[from Old French vigile, from Medieval Latin vigilia watch preceding a religious festival, from Latin: vigilance, from vigil alert, from vigēre to be lively].

Thus “surveillance” is “watchful vigilance from above”. So a literal translation of “surveillance” into English gives “overwatching” – not a real English word. The closest existing English word is the word “oversight” (dictionary.com, Random House, 2013), which emerged around the year 1300. In fact Google Translate returns the French word “surveillance” when presented with the English word “oversight”. But in current English usage, the word “oversight” has a somewhat different and in fact, double, meaning, compared with “surveillance”. Specifically, “oversight” can mean:

1. An omission or error due to carelessness. My bank statement is full of oversights. or;
2. Supervision; watchful care: a person responsible for the oversight of the organization. (Random House, 2013).

The fact that the English word “oversight” has two meanings perhaps explains why we use the French word “surveillance”, i.e. why we use the term “*surveillance cameras*” rather than “*oversight cameras*”.

A surveillance camera is a camera that typically watches from above, e.g.:

- The “eye-in-the-sky” afforded by an aerial surveillance “drone”;
- Cameras on property (real-estate), i.e. land or buildings.
 - Cameras are affixed to land by way of watchtowers or poles or masts.
 - Cameras are affixed to buildings in weatherproof enclosures, or affixed inside building interiors by way of “ceiling domes of wine-dark opacity” (Patton, 1995).

SOUSVEILLANCE

There has been a recent explosion of interest in body-borne camera systems to help people see better, as well as for body-centered sensing of the body itself and the environment around it. Such systems include the self-gesturing neckworn sensor-camera of Figure 1, when fitted also with a 3D data projector to project onto the real world (See Figure 2).

Another related invention is the MannGlass™ HDR (High Dynamic Range) welding glass that evolved out of experiments in photographically mediated visual reality in the 1970s (pre-dating 3M’s SpeedGlass™ welding glass of 1981, which only provided global auto-darkening across the whole field of view), leading eventually to the general-purpose “Digital Eye Glass” (EyeTap) (See Figure 3).

It is clear from the foregoing that a portable, wearable, or implantable camera borne by an individual person is not a surveillance camera. It is still a veillance camera, i.e. it is still “watching”

Figure 1. Neckworn lifelogging sensor-cameras. A lifelog is a lifelog (or lifelong weblog) that does not require conscious thought or effort to generate (Mann, 2001).



Figure 2. Neckworn Augmented Reality pendant comprised of a wearable camera and projector together on the pendant (Mann, 2001). The wearer can control the apparatus by self-gesturing. Mann referred to the wearable computer in this sense as a “Sixth Sense”, and used the term “Synthetic Synesthesia of the Sixth Sense” (Mann, 2001; Geary, 2003) (Source: Wikimedia Commons).



(veillance), but not necessarily “sur” (from above, physically or hierarchically).

What kind of veillance is it, though, if it is not *surveillance*? The French prefix “sur” means “on” or “over” or “above”. Its opposite is “sous” which means “under” or “below” as in “sous-chef” or “sous la table” (under the table). Thus body-borne

sensing is widely referred to as “sousveillance”, or just “veillance” (Mann, 2002; Kerr and Mann, 2006; Dennis, 2008; U.C. Berkeley, 2009; Bakir, 2010; Fletcher et al, 2011).

Sousveillance is a fundamental and universal concept that is widely understood across all ages and cultures (See Figure 4).

Figure 3. Digital Eye Glass (EyeTap) and the evolution of wearable computing in everyday life (top row). Mann's Digital Eye Glass (1999) and Google Glass (2012) (Source: Wikimedia Commons).

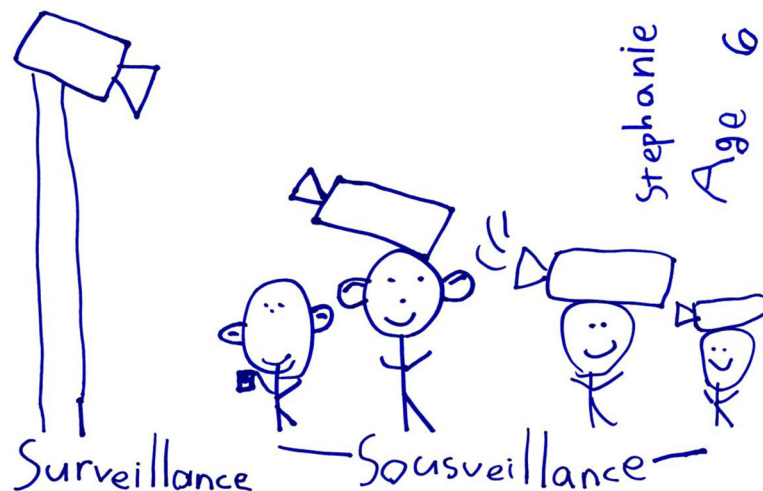


Through the Glass, Lightly



IEEE Technology and Society, Volume 31, Number 3, Fall 2012, Pages 10-14.

Figure 4. Six-year-old's drawing depicts Surveillance (overwatching) as compared with Sousveillance (underwatching). As a student in a French Immersion school, she thinks of Surveillance as the centralized veillance of large entities (governments and corporations), vs. Sousveillance as the distributed "crowdsourced" veillance of the masses == Eyes AND ears down at street level, rather than high on a watchtower or streetlight pole.



VEILLANCE INTEGRITY AND VEILLANCE HYPOCRISY

To a six-year-old who's told she's not allowed to take pictures in a place where she's surrounded by surveillance cameras, it would seem to her that property (land and buildings) has more rights than people – that property almost always has the right to bear cameras, but people often don't. She does not fully comprehend the more complex sociopolitical landscape in which it is really the unseen behind-the-scenes governments, police, and property owners who have those rights, not the land or buildings themselves. Moreover, in this day and age of AR (Augmented Reality) (Mann, 2001), the hypocrisy of one-sided veillance is accentuated by the ubiquitous appearance of 2-dimensional camera-ready QR (Quick Read) barcodes through business establishments, including those where cameras are prohibited (See Figure 5).

To the six-year old who's being taught that it is impolite to stare, how do we explain the impoliteness of the surveillance cameras all around us? The “unblinking eye” of surveillance is said to “never avert its gaze”. And if she's told to stop taking pictures, should she hide her camera and keep taking pictures? Surveillance cameras are often hidden, and if you ask a security guard or staff person what's inside those mysterious ceiling domes of wine-dark opacity, they'll usually avoid giving an honest answer. In fact the security industry often advises that cameras should be hidden, or concealed, to avoid, for example, vandalism (see for example what is happening with the Camover social movement <http://www.youtube.com/watch?v=9GCsd2TJKjQ>). If we ask whether or not we're under surveillance, a typical answer is that we're forbidden from knowing, “for security purposes”.

So should not sousveillance enjoy the same rights to secrecy? For the safety of the individual wearing a camera, should the camera not be hid-

Figure 5. Hypocrisy of surveillance: Many establishments use surveillance cameras but prohibit sousveillance. Signs in business establishments read “NO CAMERAS/VIDEO”, “NO CELL PHONES”, “NO CELL PHONE IN STORE PLEASE” – yet, ironically, a cell phone is needed to read the in-store pre-product Quick Read (QR) codes on boxes of watermelons and other merchandise displays.



den? Social movements like Camover merely amount to destruction of property, but social movements like “Stop the Cyborgs” could lead to violence against persons, not just property; violence against sousveillance can result in injury or death of a person. Is human life not worth more than physical property? And if so, should not sousveillance be granted the same, or more, “rights” to secrecy than surveillance?

Authorities who have the only recordings of incidents, including those depicting wrongdoing by the authorities, are being trusted to be keepers and curators of the only copy of evidence that might show their wrongdoing. Consider, for example, the Brazilian electrician who was shot and killed by police in a London subway, when they mistook him for someone else. A simple case of mistaken identity turned into a case of lost surveillance recordings. Police seized four separate surveillance system recordings and reported that all four systems were blank and failed to record the incident:

And now police say there are no CCTV pictures to reveal the truth. So why did plainclothes officers shoot young Jean Charles de Menezes seven times in the head, thinking he posed a terror threat?

Evidence of this hold-up should have been provided by CCTV footage from dozens of cameras covering the Stockwell ticket hall, escalators, platforms and train carriages.

However, police now say most of the cameras were not working. (Guardian 2005)

A similar situation occurred more recently, but this time with sousveillance:

On Memorial Day 2011, Narces Benoit witnessed and filmed a group of Miami police officers shooting and killing a suspect ... He was then confronted by officers who handcuffed him and smashed his cell phone, but Benoit was able to sneakily preserve

the video ... he discreetly removed the [memory] card and placed it in his mouth. (NBC News and the Miami Herald)

In this case Benoit was not sousveilling for personal gain, or even for personal safety or personal protection. He was sousveilling for the public good, and in some sense his effort was a noble one. Thus a person wearing a camera perhaps has a moral and ethical imperative to (1) record wrongdoing by authorities; and (2) to conceal the recording apparatus, and its associated functioning.

THE VEILLANCE CONTRACT ANALOGY: RECIPROCAL RECORDING RIGHTS

Whereas there may exist certain places like change rooms where recording is not appropriate, it has been suggested that in any place where surveillance is used, sousveillance must also be permitted.

The justification for such a reciprocal recording right can be understood by way of the “contract analogy” (“veillance contract analogy”).

Imagine A and B enter into a written contract but that only A has a copy of the contract. If B were to carelessly lose its copy of the contract, the contract is still valid. But if the reason B does not have a copy of the contract is that A prohibited B from having a copy, then the contract is not valid. The reason for this rule is to prevent falsification.

Let’s suppose we have a 50 page contract to which A and B both agreed, with their signatures on page 50. Later, A could go back and change page 49 (one of the non-signature pages). But if A and B both had copies, the copies would differ, and the courts would place higher scrutiny on the remaining parts, possibly examining the papers by microscope or other forensics to determine which copy was falsified.

By prohibiting these checks and balances (i.e. by prohibiting B from having a copy of the contract), A is creating a potential conflict-of-interest,

and a possibility (maybe even an incentive) for falsification of the contract.

In today's world we live a social contract of the oral and action-based variety. Much of what we do is spoken or acted out, and not written. An oral contract is still legally binding. So if one entity insists on having the only copy of what was said or agreed upon, A is creating the possibility to falsify (whether by editing or simply by omission, i.e. by deleting some pictures and keeping others) the recorded evidence.

Such a monopoly on sight can create "surveillance curation", i.e. the person doing the surveillance "curates reality" by selecting certain "exhibits" to keep, and others to delete.

In response to such a proposal, Paul Banwatt, a lawyer at Gilbert's LLP, has suggested that:

1. Surveillance cannot be secret, or else individuals will be unable to tell when their right exists, or if one assumes the right is assumed to exist then; and
2. Those who sousveil must be informed that they are NOT being recorded in order to form the necessary basis for a demand to stop sousveillance. (Personal communication by way of author S. Mann's Veillance Group on LinkedIN.com).

A practical solution to this problem is to at least agree that when a person is prohibited from recording their own side of an interaction (i.e. prohibited from recording their own senses), the person who prohibited should have their side also removed from admissibility in any court of law. Such a "veillance contract" does not require either party to know whether or not their actions are being recorded!

Under the proposed rule, an organization installing a "no photography" sign, or otherwise discouraging people from keeping their own copy of the "veillance contract", would make their own surveillance recordings inadmissible in a court of law.

DEFINING SUR/SOUSVEILLANCE

The higher you look up the ladder, the more difficult it becomes to tell the good guys from the bad guys. — Reese, Person of Interest

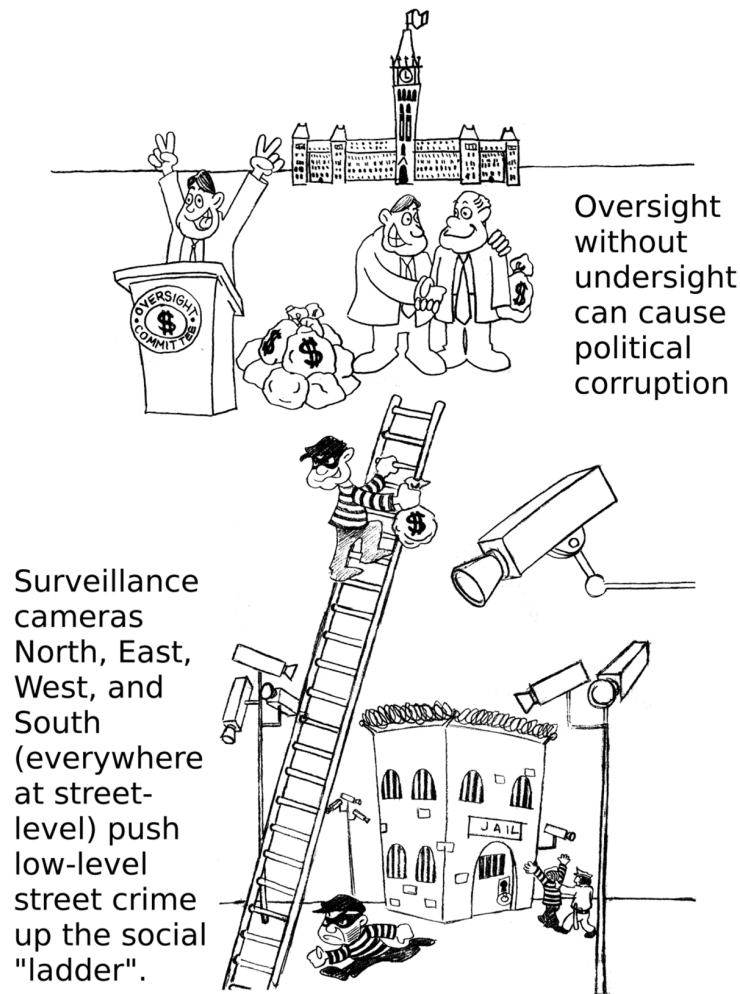
Surveillance is the veillance of large entities in a position of authority, whereas sousveillance is the veillance of smaller entities not in a position of authority (Mann, 2002; Kerr and Mann, 2006). And to the extent that authorities want to watch, but not be watched, the veillance of authority – surveillance – has, associated with it, an inherent conflict-of-interest.

As mentioned previously, a simple and often-used definition of surveillance is cameras borne by property (land or buildings), and of sousveillance is cameras borne by people. But a hierarchical definition is also possible: surveillance is the veillance of large powerful entities on the higher rungs of the social "ladder", and sousveillance is the veillance of the masses on the lower rungs of the social "ladder". This leads to obvious problems with conflict-of-interest and possible corruption (See Figure 6). It is often said that putting surveillance cameras in one part of a city will merely "move" or "push" crime away to other parts of the city. But putting cameras everywhere down at street-level gives crime nowhere to "move" but up the social ladder toward corruption.

Moreover, not only can surveillance cameras "push" crime "up", but they can also be used to perpetrate crimes. Authorities can use surveillance cameras to determine when someone is away (notifying accomplice robbers), or use surveillance cameras to stalk a victim:

A SECURITY guard at one of Edinburgh's best-known visitor attractions used CCTV cameras to stalk a young female worker and spy on the public. James Tuff used the camera system at Our Dynamic Earth, Edinburgh, to track his victim and then radio her with lewd comments.

Figure 6. The “Ladder Theory” of Veillance. A society with surveillance-only (i.e. where sousveillance is prohibited) is a society in which there is an inherent conflict-of-interest that tends to favour higher-level corruption over low-level street crime (i.e. tends to “push” or “move” crime from being under veillance to rising above the veillance).



He even trained the cameras on members of the public milling about outside, in one case saving footage of two girls kissing to show to colleagues.

Tuff eventually sexually assaulted Dora Alves... He was fined and placed on the sex offenders register for three years. ... She said: ‘At first it was just the odd comment about my body; he would say things about me having a real woman’s body... But soon after he would appear out of nowhere when I was cleaning in the toilets. ...’ as she walked to the canteen on her break and stopped to collect

something from her locker. ‘Mr Tuff came out of his office and grabbed me from behind. ...’ She said CCTV footage which could have proved the incident took place had gone missing. (News Scotsman.com. ‘Cleaner says she was stalked on CCTV by security guard’, March 2011)

Thus there is obviously a conflict-of-interest among higher authorities that can give rise to an incentive to promote surveillance while prohibiting sousveillance.

This gives us a possible definition for *sousveillance*:

- **Surveillance:** Is the *veillance* of authority, i.e. the *veillance* that can be used with a prohibition on other *veillances*, i.e. one entity conducting surveillance can (and sometimes does) prohibit other entities from conducting *veillance*;
- **Sousveillance:** Is the *veillance* of non-authority, i.e. the *veillance* of the masses. One person conducting *sousveillance* cannot prohibit others from conducting *veillance*.

In other words, surveillance can be *defined* as the *veillance* of hypocrisy (i.e. “we’re watching you but you’re not allowed to watch us”).

The antonym of hypocrisy is integrity. Thus, by mere logic, *sousveillance*, being the opposite of surveillance, is the *veillance* of integrity. Suppose we accept simply that “surveillance is the *veillance* of integrity”? Let us “unpack” this definition in the following way: to the extent that *veillance* is the collection of data, we might consider data integrity. One of the best ways that computers ensure data integrity is through redundancy. For example, data integrity on computer disks is best ensured through such technologies as RAID (Redundant Array of Independent Disks, formerly known as “Redundant Array of Inexpensive Disks”).

Sousveillance is analogous to RAID, in the sense that it is a Redundant Array of Independent *Veillances*, i.e. we could abbreviate it as “RAIV”. A RAIV is therefore a possible way of ensuring *veillance* integrity through a decentralized *veillance*.

Consider, for example, a situation in which any member of a society can commit an act of wrongdoing. Centralized *veillance* would allow the possibility of wrongdoing by an authority to falsify self-incriminating *veillance* data, whereas distributed *veillance* is less likely to fall totally under the control of a single entity that might falsify the data.

The opposite of integrity, when referring to human-nature, is hypocrisy. The opposite of integrity when referring to data is corruption, i.e. “data corruption” is the opposite of “data integrity” (See Table 1).

We can think of a *sousveillance* device as an integrity device, e.g. as eyeglass, the device might be presented or marketed or understood as an “honesty glass”, or as a pendant, it might become an “honesty pendant”.

DATAVEILLANCE

Roger Clarke has produced a seminal body of work on the topic of “dataveillance” which he describes as a portmanteau of “data” and “surveillance” (Clarke, 1998, 1999). We can generalize this concept as follows:

There is no antonym to “Data” in the dictionary, but if we go from its Latin meaning of “given”, then its opposite would or could be “taken”.

But “data” is part of a well-known hierarchy: data, information, knowledge, wisdom, and all but “data” have previously defined opposites (See Table 2).

Thus, putting *Veillance* in the middle, *Sur* above, *Sous*, under, and *Data* beside it, we have “Dataveillance”, “Infoveillance”, “Knowveillance”, and “Wisdomveillance” offset by their opposites.

Table 1. Hypocrisy of surveillance, when it becomes (or is defined as) theveillance of a single entity (i.e. the “authority”) that prohibits otherveillances, as compared to the integrity of distributedveillance

	Surveillance (Centralized)	Sousveillance (Distributed)
Human-nature	Hypocrisy	Integrity (RAIV)
Data	Corruption	Integrity (RAID)

Table 2. “DI KNOWise” veillances

Understanding	“Overstanding”	Veillance
Data	Taken	Dataveillance
Information	Misinformation	Infoveillance
Knowledge	Ignorance	“Knowveillance”, “Knoveillance”, “Knowleveillance”
Wisdom	Stupidity	“Wisdomveil- lance” (“Wisdoveillance”, “Wisveillance”)

UBERVEILLANCE

The seminal work of M.G. Michael and K. Michael define the concept of Uberveillance as embedded surveillance (Masters & Michael, 2005; Masters & Michael, 2007; Michael et al., 2008; Michael & Michael, 2007; Michael & Michael, 2009; Michael & Michael, 2010; Perusco & Michael 2007). The definition appears in some dictionaries, e.g. “An omnipresent form of 24/7 surveillance of humans based on widespread electronic devices, and especially computer chips embedded into bodies.” – Wiktionary.

Table 3 outlines the etymology of Uberveillance in the context of its language mixtures.

As veillance encroaches closer on the body, this research on Uberveillance highlights the dangers faced by a corporeal technology that itself becomes more like surveillance than sousveillance.

Table 3. Veillances in 3 languages, French, German, English

French	Sur	Sous	Veillance
German	Über	Unter	Wachung
English	Over	Under	Watching (monitoring, sight)

FROM CROWD VEILLANCE TO CLOUD VEILLANCE: GOVERNANCE OF THE GOOLAG, OR GAOLBROKEN GOOGLASS?

The recent introduction of Google Glass has suggested a possible reversal of sousveillance, i.e. what happens when sousveillance is commercialized by a large corporation that re-centralizes what was formerly a distributed form of computation, sensing, and “crowd veillance”.

Google has decided that it will pre-approve all apps offered to glasses users, unlike its more wide open market for Android phones and tablets. ‘It’s so new, we decided to be more cautious,’ Schmidt said. ‘It’s always easier to open it up more in the future.’ (Reuters, ‘Google’s Schmidt says talking to glasses can be weird, inappropriate’ Reporting by Aaron Pressman; Editing by Lisa Shumaker, Reuters, Thu Apr 25, 2013 6:21pm EDT, <http://www.reuters.com/article/2013/04/25/us-google-harvard-idUSBRE93O1FF20130425>

Google has also threatened to remotely sabotage anyone’s eyeglass if they sell it or even lend it to others. This remote self-destruct and sabotage capability is built into the product.

This “deconomics” (“sabotage economics”), at the hardware level, suggests a form of centralized control rather than the freedom envisioned for sousveillance. Thus it has been questioned whether Google’s vision is one of sousveillance or surveillance (Corey Manders, IEEE ISTAS13, Toronto, Ontario, Canada, 2013 June 28).

Table 4. Corporeality vs. existentiality

		Corporeality	
Existentiality	Low	Surveillance	Uberveillance
	High	??? (“Unterveillance”)	Sousveillance

We might therefore consider the “Wearability” (Corporeality) and Existentiality axes as suggested in “Can Humans Being Clerks make Clerks be Human? - Exploring the Fundamental Difference between UbiComp and WearComp”, by S. Mann, in Oldenbourg Electronic Journals, ISSN 0944-2774, Informationstechnik und Technische Informatik, Volume 43, Issue 02, pages 97-106 <http://wearcam.org/itti/>

If we put Uberveillance on these axes, we see a missing quadrant (See Table 4) which we might call “unterveillance”.

UNTERVEILLANCE

Just as sousveillance can be co-opted by a large corporation, we might ask the question, “can surveillance also be reversed”? For example, what if the video captured by cameras in the environment (e.g. cameras on land and buildings) could become “existential”, i.e. distributed, rather than monopolized.

This suggests that it is possible to have a reversal of surveillance, e.g. the new camera-based streetlights could catch a corrupt police chief or mayor, as easily as they might capture a robber or lone thief.

CONCLUSIONS

In this chapter we have considered Veillance (Sur and Sous), and Uberveillance (the corporatization or over-governance of sousveillance). Recent developments suggest a possible reversal of sousveillance into uberveillance, and surveillance into unterveillance.

Much needs to be explored, but one thing is certain: we have moved from living in a “surveillance society” to living in a “veillance society” where there is a plurality of veillances, not just one!

REFERENCES

- Bakir, V. (2010). *Sousveillance, media and strategic political communication*. London, UK: Continuum.
- Burgess, J. G., Warwick, K., Ruiz, V., Gasson, M. N., Aziz, T. Z., Brittain, J., & Stein, J. (2010). Identifying tremor-related characteristics of basal ganglia nuclei during movement in the Parkinsonian patient. *Parkinsonism & Related Disorders*, 16(10), 671–675. doi:10.1016/j.parkreldis.2010.08.025 PMID:20884273
- Choney, S. (2011). *NBC news*. Retrieved from <http://www.nbcnews.com/technology/technology/memory-card-mouth-saves-police-shooting-video-122903>
- Clarke, R. (1988). Information technology and dataveillance. *Communications of the ACM*, 31(5), 498–512. doi:10.1145/42411.42413
- Clarke, R. (1999). *Introduction to dataveillance and information privacy, and definitions of terms*. Roger Clarke’s Dataveillance and Information Privacy Pages.
- Dennis, K. (2008). Viewpoint: Keeping a close watch—the rise of self-surveillance and the threat of digital exposure. *The Sociological Review*, 56(3), 347–357. doi:10.1111/j.1467-954X.2008.00793.x
- Fletcher, G., Griffiths, M., & Kutar, M. (2011). *A day in the digital life: A preliminary sousveillance study*. Retrieved from <http://ssrn.com/abstract=1923629>
- Foster, K. R., & Jaeger, J. (2007). RFID inside. *IEEE Spectrum*, 44, 24–29. doi:10.1109/MSPEC.2007.323430
- Gasson, M. N., Hutt, B. D., Goodhew, I., Kyberd, P., & Warwick, K. (2005b). Invasive neural prosthesis for neural signal detection and nerve stimulation. *International Journal of Adaptive Control and Signal Processing*, 19(5), 365–375.

- Gasson, M. N., Wang, S. Y., Aziz, T. Z., Stein, J. F., & Warwick, K. (2005a). Towards a demand driven deep-brain stimulator for the treatment of movement disorders. In *Proceedings of 3rd IEE International Seminar on Medical Applications of Signal Processing*, London, UK: IEE.
- Geary, J. (2003). *The body electric: An anatomy of the new bionic senses*. New Brunswick, NJ: Rutgers University Press.
- Hameed, J., Harrison, I., Gasson, M. N., & Warwick, K. (2010). A novel human-machine interface using subdermal magnetic implants. In *Proceedings of the IEEE International Conference on Cybernetic Intelligent Systems*. IEEE.
- Hayes, A. (2013). Cyborg cops, googlers, and connectivism. *IEEE Technology and Society*, 32(1), 23–24. doi:10.1109/MTS.2013.2247731
- Kerr, I., & Mann, S. (2006). *Exploring equiveillance*. Retrieved from http://www.anonequity.org/weblog/archives/2006/01/exploring_equiv_1.php
- Lyon, D. (2001). *Surveillance society*. Buckingham, UK: Open University Press.
- Mann, S. (2001). *Intelligent image processing*. New York: John Wiley-IEEE Press. doi:10.1002/0471221635
- Mann, S. (2002). Sousveillance, not just surveillance. *Metal and Flesh*, 6(1).
- Masters, A., & Michael, K. (2005). Humancentric applications of RFID implants: The usability contexts of control, convenience and care. In *Proceedings of Mobile Commerce and Services*. IEEE. doi:10.1109/WMCS.2005.11
- Masters, A., & Michael, K. (2007). Lend me your arms: The use and implications of human-centric RFID. *Electronic Commerce Research and Applications*, 6(1), 29–39. doi:10.1016/j.elerap.2006.04.008
- Michael, K., & Clarke, R. (2013). Location and tracking of mobile devices: Überveillance stalks the streets. *Computer Law and Security Review*, 29(2).
- Michael, K., & Michael, M. G. (2008). *Innovative automatic identification and location-based services: From bar codes to chip implants*. Hershey, PA: IGI Global.
- Michael, K., & Michael, M. G. (2009). *Innovative automatic identification and location-based services: From bar codes to chip implants*. Hershey, PA: IGI Global. doi:10.4018/978-1-59904-795-9
- Michael, M. G., Fusco, S. J., & Michael, K. (2008). A research note on ethics in the emerging age of überveillance. *Computer Communications*, 31(6), 1192–1199. doi:10.1016/j.comcom.2008.01.023
- Michael, M. G., & Michael, K. (2007). A note on überveillance. In *From dataveillance to uberveillance and the realpolitik of the transparent society*. Wollongong, Australia: Academic Press.
- Michael, M. G., & Michael, K. (2010). Toward a state of überveillance. *IEEE Technology and Society Magazine*, 29(2), 9–16. doi:10.1109/MTS.2010.937024
- Patton, P. (1995). Caught-You used to watch television: Now it watches you. *Wired*, 3(1), 124–127.
- Perusco, L., & Michael, K. (2007). Control, trust, privacy, and security: Evaluating location-based services. *IEEE Technology and Society Magazine*, 26(1), 4–16. doi:10.1109/MTAS.2007.335564
- Thompson, T., & Phillips, T. (2005). *Death in Stockwell: The unanswered questions*. Retrieved from <http://www.guardian.co.uk/uk/2005/aug/14/july7.terrorism>
- UC Berkeley School of Information. (2009). *Info 290: Surveillance, sousveillance, coveillance, and dataveillance*. Retrieved from <http://www.ischool.berkeley.edu/courses/i290-sscd>

Warwick, K., Gasson, M. N., Hutt, B., Goodhew, I., Kyberd, P., & Andrews, B. et al. (2003). The application of implant technology for cybernetic systems. *Archives of Neurology*, 60(10), 1369–1373. doi:10.1001/archneur.60.10.1369 PMID:14568806

KEY TERMS AND DEFINITIONS

Access Control: In information security, access control is the selective restriction of access to a place or other resource.

Advocacy: Is considered a political process usually by a group of people with the aim to influence public-policy. An advocate is usually affiliated with a non-government organisation, undertaking media campaigns, public speaking, commissioning and publishing research.

Behaviour: Is the range of actions undertaken by a human in their physical or non-physical environment. It is the response of the system or organism to various stimuli or inputs, whether internal or external, conscious or subconscious, overt or covert, and voluntary or involuntary.

Biometrics: The measurement of physical characteristics or traits, such as fingerprints, handprints, DNA, iris or retinal patterns, gait or voice recognition for use in verifying the identity of individuals.

Chilling Effect: A discouraging or deterring effect, usually resulting from a restrictive law or regulation. For example, introducing ID scanners at licensed venues to minimize patron violence, or even introducing a curfew on a particular zone.

Ethics: A set of principles of right conduct. The rules or standards governing the conduct of a person or the members of a profession.

Geographic Information Systems: A computer application used to store, view, and analyze geographical information, especially maps. A GIS can contain both vector and raster images.

Google Glass: A digital glass head up display (HUD) device that carries many smartphone functions. Its capabilities include identifying current locations (augmented reality), voice and video calls, GPS navigation, sending/receiving messages, taking notes, as well as snapping and sharing photos and video.

Harm: To cause physical or psychological injury or damage.

Human Cloud: The emerging cloud revolutionised by wearable technologies, allegedly making users feel more intelligent and in control of their lives.

Identity Cards: An identity document (also called a piece of identification, ID, or colloquially as one's 'papers') is any document which may be used to verify aspects of a person's personal identity. If issued in the form of a small, mostly standard-sized card, it is usually called an identity card (IC). Countries which do not have formal identity documents may require informal documents.

Chip Implants: A medical device manufactured to replace a missing biological function or to enhance an existing one. Medical implants are man-made devices made of a biomedical material such as titanium, silicone or apatite. In some cases implants contain electronics e.g. artificial pacemaker and cochlear implants. Some implants are bioactive, such as subcutaneous drug delivery devices in the form of implantable pills or drug-eluting stents.

iPlant: Is the potential for an invention of an Internet-enabled chip implant required to login to online applications. The word "iPlant" conjoins the words "internet" and "implant" and is a play on the internet-based applications developed by Apple Inc. and NTT Docomo (e.g. iTunes, iPod, iLife, iSight, iPhone, iPad, imode, i-shot, and iD).

Interdisciplinary: Of, relating to, or involving two or more academic disciplines that are usually considered distinct.

Legislation: A proposed or enacted law or group of laws.

Lifeloggers: Wear body-worn video recorders in order to capture their entire lives digitally, or large portions of their lives.

National Security: A collective term encompassing both national defense and foreign relations. Internationally has been used to denote an all-hazards approach to security, ensuring the safety of the citizen.

Omnipresent: Present everywhere simultaneously.

Omniscience: Having total knowledge; knowing everything.

Pacemakers: Any of several usually miniaturized and surgically implanted electronic devices used to stimulate or regulate contractions of the heart muscle.

Profiling: To draw or shape a profile of an individual. Increasingly proactive profiling in real-time is occurring, especially in shopping malls, using consumer-owned mobile phones.

Nanotechnology: The science and technology of building devices, such as electronic circuits, from single atoms and molecules.

Regulation: The act of regulating or the state of being regulated. A principle, rule, or law designed to control or govern conduct.

Smart Dust: Is a system of many tiny micro electromechanical systems (MEMS) such as sensors, robots, or other devices, that can detect, for example, light, temperature, vibration, magnetism, or chemicals.

Social Policy: A policy for dealing with social issues.

StreetView: Google Street View is a technology featured in Google Maps and Google Earth that provides panoramic views from positions along many streets in the world. It was launched on May 25, 2007, in several cities in the United States, and has since expanded to include cities and rural areas worldwide.

Transhumanism: (Abbreviated as H+ or h+) Is an international cultural and intellectual movement with an eventual goal of fundamentally transforming the human condition by developing and making widely available technologies to greatly enhance human intellectual, physical, and psychological capacities.

Value Chain: A chain of activities that a firm operating in a specific industry performs in order to deliver a valuable product or service for the market. Can also be considered a chain of firms required to offer a complex service.

Wearable Computers: Also known as body-borne computers are miniature electronic devices that are worn by the bearer under, with or on top of clothing. This class of wearable technology has been developed for general or special purpose information technologies and media development. Wearable computers are especially useful for applications that require more complex computational support than just hardware coded logics.